IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI

RACHEL TAYLOR and TRAVIS TAYLOR, individually, and on behalf of all others similarly situated, Plaintiffs, v. CLAY-PLATTE FAMILY MEDICINE CLINIC, P.C., SUMMIT FAMILY AND SPORTS MEDICINE, COBBLESTONE FAMILY MEDICINE CLINIC, and BARRY POINTE FAMILY CARE, LLC, Defendants.	Case No. _____ **CLASS REPRESENTATION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Rachel Taylor and Travis Taylor (collectively, "Plaintiffs"), individually, and on behalf of all others similarly situated, bring this action against the Clay-Platte Family Medicine Clinic, P.C., Summit Family and Sports Medicine, Cobblestone Family Medicine, and Barry Pointe Family Care, LLC (the "Clinics" or "Defendants"). Plaintiffs bring this action by and through their attorneys, and allege, based upon personal knowledge as to their own actions, and based upon information and belief and reasonable investigation by their counsel as to all other matters, as follows.

I. INTRODUCTION

1. The Clinics are affiliated medical service providers that operate in the state of Missouri. The Clinics share patients and patient information. Plaintiffs and the putative Class are current and former patients of the Clinics.

2. As part of their operations, the Clinics collect, maintain, and store highly sensitive personal and medical information belonging to their patients, including, but not limited to such as

full names, Social Security numbers, dates of birth, addresses, and contact information ("personally identifying information" or "PII") as well as Private Health Information ("PHI") including health insurance information (collectively with PII, "Private Information").

3. On or before June 26, 2024, the Clinics experienced a data breach incident in which unauthorized cybercriminals accessed their information systems and databases and stole Private Information belonging to Defendants' current and former patients (the "Data Breach"). The Clinics discovered this unauthorized access on June 26, 2024. On September 10, 2024, the Clinics identified all individuals whose information was compromised in the Data Breach.

4. On or about October 16, 2024, the Clinics sent a notice to individuals whose information was accessed in the Data Breach.

5. Because the Clinics stored and handled Plaintiffs' and Class members' highly-sensitive Private Information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

6. Ultimately, the Clinics failed to fulfill this obligation, as unauthorized cybercriminals breached their information systems and databases and stole vast quantities of Private Information belonging to their patients, including Plaintiffs and Class members. The Data Breach—and the successful exfiltration of Private Information—were the direct, proximate, and foreseeable results of multiple failings on the part of the Clinics.

7. The Data Breach occurred because the Clinics failed to implement reasonable security protections to safeguard its information systems and databases. Further, and upon information and belief, there existed an unreasonable delay between the Data Breach and when the Clinics discovered the Breach on June 26, 2024. Moreover, before the Data Breach occurred, the Clinics failed to inform the public that its data security practices were deficient and inadequate.

Had Plaintiffs and Class members been made aware of this fact, they would have never provided such information.

8. The Clinics' subsequent handling of the breach was also deficient. Critically, after discovering the Breach, the Clinics delayed for over three months before they sent notice to inform affected individuals.

9. As a result of the Clinics' negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiffs and Class members suffered injuries, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;
- Charges and fees associated with fraudulent charges on their accounts; and
- The continued and increased risk of compromise to their Private Information, which remains in the Clinics' possession and is subject to further unauthorized disclosures so long as the Clinics fail to undertake appropriate and adequate measures to protect their Private Information.

10. Accordingly, Plaintiffs bring this action on behalf of all those similarly situated to seek relief for the consequences of the Clinics failure to reasonably safeguard Plaintiffs' and Class members' Private Information; its failure to reasonably provide timely notification to Plaintiffs and Class members that their Private Information had been compromised; and for the Clinics'

failure to inform Plaintiffs and Class members concerning the status, safety, location, access, and protection of their Private Information.

II. PARTIES

Plaintiff Rachel Taylor

11. Plaintiff Rachel Taylor is a resident and citizen of Kansas City, Missouri. Plaintiff Rachel Taylor is a patient of Clay-Platte Family Medicine. Plaintiff Rachel Taylor received the Clinics' Data Breach Notice.

Plaintiff Travis Taylor

12. Plaintiff Travis Taylor is a resident and citizen of Kansas City, Missouri. Plaintiff Travis Taylor is a patient of Clay-Platte Family Medicine. Plaintiff Travis Taylor received the Clinics' Data Breach Notice.

Defendant Clay-Platte Family Medicine Clinic, P.C.

13. Defendant Clay-Platte Family Medicine Clinic, P.C. is a Missouri professional corporation with its principal place of business located at 5501 NW 62nd Terrace, Kansas City, Missouri.

Defendant Summit Family and Sports Medicine

14. Defendant Summit Family and Sports Medicine is a medical clinic with its principal place of business located at 3601 NE Ralph Powell Road, Lee's Summit, Missouri.

Defendant Cobblestone Family Medicine Clinic

15. Defendant Cobblestone Family Medicine Clinic is a medical clinic with its principal place of business located at 1133 W Kansas Street, Liberty, Missouri.

Defendant Barry Pointe Family Care, LLC

16. Defendant Barry Pointe Family Care, LLC is a Missouri limited liability company with its principal place of business at 9151 NE 81st Terrace, Kansas City, Missouri.

III. JURISDICTION AND VENUE

17. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from the Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

18. This Court has personal jurisdiction over the Defendants because they are headquartered in Missouri.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' and Class members' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. The Clinics – Background

20. The Clinics are affiliated health care service providers that operate throughout Missouri. The entities freely share patients and patient information with each other and, upon information and belief, operate off the same information technology and network architecture. As part of their normal operations, the Clinics collect, maintain, and store large volumes of Private Information belonging to their current and former patients.

21. Upon information and belief, the Clinics failed to implement necessary data security safeguards at the time of the Data Breach. This failure resulted in cybercriminals accessing the Private Information belonging to their current and former patients—Plaintiffs and Class members.

22. Current and former patients of the Clinics, such as Plaintiffs and Class members, made their Private Information available to the Clinics with the reasonable expectation that any entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. They similarly expected that, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

23. This expectation was objectively reasonable and based on an obligation imposed on the Clinics by statute, regulations, industrial custom, and standards of general due care.

24. Unfortunately for Plaintiffs and Class members, the Clinics failed to carry out their duty to safeguard sensitive Private Information and provide adequate data security. As a result, they failed to protect Plaintiffs and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

25. According to the Clinics' public statements, on June 26, 2024, the Clinics discovered suspicious activity on their network environment. Subsequent investigation determined that cybercriminals had breached the Clinics' information and acquired files containing their patients' Private Information.

26. By September 10, 2024, the Clinics had identified the individuals whose Private Information was compromised in the Breach.

27. On and around October 16, 2024, the Clinics sent notice of the Data Breach to all individuals affected by this data security incident.

28. The Clinics estimate that the Private Information belonging to over 53,000 individuals was compromised in this incident.

29. Omitted from the notice were the date that the cybercriminal first obtained access to Defendants' systems, the length of time the cybercriminals had access to Defendants' systems, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class members, who retain a vested interest in ensuring that their Private Information remains protected.

30. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

31. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

32. The attacker accessed and acquired files in Defendants' computer systems containing unencrypted Private Information of Plaintiffs and Class members, including their names, addresses, dates of birth, Social Security numbers, PHI, and other sensitive information. Plaintiffs' and Class members' Private Information was accessed and stolen in the Data Breach.

33. Plaintiffs further believe that their Private Information and that of Class members was or will be sold on the dark web, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

C. The Clinics' Many Failures Both Prior to and Following the Breach

34. The Clinics collect and maintain vast quantities of Private Information belonging to Plaintiffs and Class members as part of their normal operations. The Data Breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of the Clinics.

35. First, the Clinics inexcusably failed to implement reasonable security protections to safeguard their information systems and databases.

36. Second, upon information and belief, the Clinics failed to timely detect this data breach with the Clinics' computer systems. This delayed detection provided these cybercriminals with days or weeks during which they could freely access and steal the sensitive Private Information belonging to the Clinics' patients.

37. Third, the Clinics failed to inform the public that their data security practices were deficient and inadequate. Had Plaintiffs and Class members been aware that the Clinics did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to the Clinics.

38. In addition to the failures that lead to the successful breach, the Clinics' failings in handling the breach and responding to the incident exacerbated the resulting harm to the Plaintiffs and Class members.

39. The Clinics' inexcusable three-month delay before informing victims of the Data Breach that their Private Information was compromised virtually ensured that the cybercriminals who stole this Private Information could monetize, misuse and/or disseminate that Private Information before the Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the

substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

40. In short, the Clinics' myriad failures, including the failure to timely detect an intrusion and failure to timely notify Plaintiffs and Class members that their personal and medical information had been stolen due to the Clinics' security failures, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiffs' and Class members' Private Information months before the Clinics finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

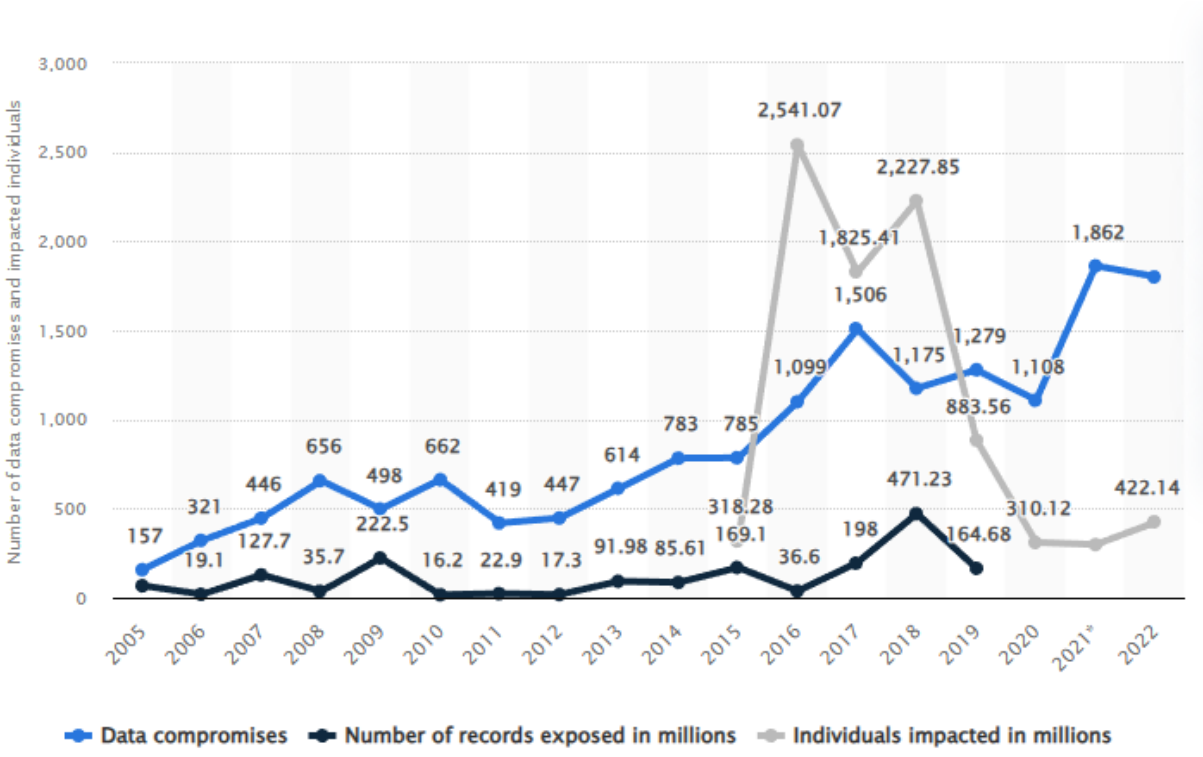
41. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, and Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

42. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[1] The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just 8 shy of the record of 715 set in 2021 and still double that of the number of similar such compromises in 2017 and triple the number of compromises in 2012.[2]

43. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data

[1] *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report.
[2] *2022 Healthcare Data Breach Report*, The HIPAA Journal (January 24, 2023), available at: https://www.hipaajournal.com/2022-healthcare-data-breach-report/.

breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.[3] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.[4]



44. This stolen PII is then routinely traded on dark web black markets as a simple commodity, with social security numbers being so ubiquitous to be sold at as little as $2.99 apiece and passports retailing for as little as $15 apiece.[5]

45. In addition, the severity of the consequences of a compromised social security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory

[3] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, Statista, available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
[4] *Id.*
[5] *What is your identity worth on the dark web?* Cybernews (September 28, 2021), available at: https://cybernews.com/security/whats-your-identity-worth-on-dark-web/.

groups can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> [a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[6]

This is exacerbated by the fact that the problems arising from a compromised social security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[7]

46. The most sought after and expensive information on the dark web are stolen medical records which command prices from $250 to $1,000 each.[8] Medical records are considered the most valuable because unlike credit cards, which can easily be canceled, and social security numbers, which can be changed, medical records contain "a treasure trove of unalterable

---

[6] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[7] *Id.*

[8] Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (January 26, 2021), available at: https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.

data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[9] With this bounty of ill-gotten information, cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.[10] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.[11] Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.[12]

47. The wrongful use of compromised medical information is known as medical identity theft and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of $13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[13] It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.[14]

48. Instances of Medical identity theft have grown exponentially over the years from approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold increase in the crime.[15]

---

[9] *Id.*
[10] *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), available at https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare. *See also* Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (August 25, 2016), available at https://www.consumerreports.org/health/medical-identity-theft-a1699327549/.
[11] *Id.*
[12] *Id.*
[13] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.
[14] *Id.*
[15] *Id.*

49. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like the Clinics charged with maintaining and securing patient PII should know the importance of protecting that information from unauthorized disclosure. Indeed, the Clinics knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[16]

50. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like the Clinics on notice of their obligation to safeguard customer and patient information.[17]

51. Given the nature of the Clinics' Data Breach, as well as the length of the time the Clinics' networks were breached and the long delay in notification to victims thereof, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class members' Private Information can easily obtain Plaintiffs' and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

52. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

[16] *See, e.g.*, *Healthcare Data Breach Statistics*, HIPAA Journal, available at: https://www.hipaajournal.com/healthcare-data-breach-statistics.
[17] *See, e.g.*, *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).

breach, because credit card victims can cancel or close credit and debit card accounts.[18] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

53. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, the Clinics failed to take appropriate steps to protect the Private Information of Plaintiffs and Class members from misappropriation. As a result, the injuries to Plaintiffs and Class members were directly and proximately caused by the Clinics' failure to implement or maintain adequate data security measures for its current and former patients.

E. The Clinics Have a Duty and Obligation to Protect Private Information

54. The Clinics have an obligation to protect the Private Information belonging to Plaintiffs and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and medical records. Plaintiffs and Class members provided, and the Clinics obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. HIPAA Requirements and Violation

55. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the

[18] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1. *See also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/.

confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq*.

56. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . . ." 45 CFR § 164.402.

57. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires entities to provide notice of a data breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

58. The Clinics failed to implement and/or maintain procedures, systems, and safeguards to protect the Private Information belonging to Plaintiffs and Class members from unauthorized access and disclosure.

59. Upon information and belief, the Clinics' security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information the Clinics create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by their workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

60. Upon information and belief, the Clinics also failed to store the information it collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

61. The Clinics also violated the HIPAA Breach Notification Rule since they did not inform Plaintiffs and Class members about the breach until over three months after it first discovered the breach.

2. FTC Act Requirements and Violations

62. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for

consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

63. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[19] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[20] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[21] The Clinics clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

64. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

[19] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed August 15, 2023).
[20] *Id.*
[21] *Id.*

65. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

67. As evidenced by the Data Breach, the Clinics failed to properly implement basic data security practices. The Clinics' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

68. The Clinics were fully aware of their obligation to protect the Private Information of its current and former patients, including Plaintiffs and Class members. The Clinics are sophisticated and technologically savvy business that relies extensively on technology systems and networks to maintain its practice, including storing its patients' PII, protected health information, and medical information in order to operate its business.

69. The Clinics had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between the Clinics and Plaintiffs and Class members. The Clinics alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiffs' and Class members' Private Information.

3. Industry Standards and Noncompliance

70. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

71. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information, like the Clinics, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, they failed to follow some or all of these industry best practices.

72. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, the Clinics failed to follow these cybersecurity best practices.

73. The Clinics should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

74. The Clinics failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

F. Plaintiffs and the Class Suffered Harm Resulting from the Data Breach

75. Like any data hack, the Data Breach presents major problems for all affected.[22]

76. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[23]

77. The ramifications of the Clinics' failure to properly secure Plaintiffs' and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

78. According to data security experts, one out of every four data breach notification recipients become a victim of identity fraud.

79. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

80. Accordingly, the Clinics' wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the

[22] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.
[23] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

scholarly journal *Preventive Medicine Reports*, public and corporate data breaches correlate to an increased risk of identity theft for victimized consumers.[24] The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[25]

81. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

82. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being $4.45 million dollars in 2023.[26] The average cost to resolve a data breach involving health information, however, is more than double this figure at $10.92 million.[27]

83. The theft of medical information, beyond the theft of more traditional forms off PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years and this explosive growth far outstrips the increase in incidence of traditional identity theft.[28] Medical Identity Theft is especially nasty for victims because of the lack of laws that limit a victim's liabilities and damages from this

[24] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.
[25] *Id.*
[26] *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds.
[27] *Id.*
[28] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.

type of identity theft (e.g., a victim's liability for fraudulent credit card charges is capped at $50), the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average, $13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.[29]

84. Here, due to the Breach, Plaintiffs and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with time spent to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite the Defendants' delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiffs' and Class members' privacy.

[29] *Id.*

85. Plaintiffs and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals.

86. As a direct and proximate result of the Clinics' acts and omissions in failing to protect and secure Private Information, Plaintiffs and Class members have been placed at a substantial risk of harm in the form of identity theft, and they have incurred and will incur actual damages in an attempt to prevent identity theft.

87. Plaintiffs retain an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Private Information was accessed in the Data Breach.

G. EXPERIENCES SPECIFIC TO PLAINTIFFS

Plaintiff Rachel Taylor

88. Plaintiff Rachel Taylor is a patient of the Defendants.

89. Plaintiff Rachel Taylor received the Clinics' data breach notice dated October 16, 2024. The notice informed Plaintiff Rachel Taylor that her Private Information was improperly accessed and obtained by third parties.

90. After the Data Breach, Plaintiff Rachel Taylor experienced a dramatic increase in the number of spam emails, calls, and text messages.

91. As a result of the Data Breach, Plaintiff Rachel Taylor has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Rachel Taylor has spent this time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

92. As a result of the Data Breach, Plaintiff Rachel Taylor has suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her Private Information for purposes of identity theft and fraud. Plaintiff Rachel Taylor is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

93. Plaintiff Rachel Taylor suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that the Clinics obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

94. As a result of the Data Breach, Plaintiff Rachel Taylor anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Travis Taylor

95. Plaintiff Travis Taylor is a patient of Defendants.

96. Plaintiff Travis Taylor received the Clinics' data breach notice dated October 16, 2024. The notice informed Plaintiff Travis Taylor that his Private Information was improperly accessed and obtained by third parties.

97. After the Data Breach, Plaintiff Travis Taylor experienced a dramatic increase in the number of spam emails, calls, and text messages.

98. As a result of the Data Breach, Plaintiff Travis Taylor has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Travis Taylor has spent this time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including, but not limited to, work and recreation.

99. As a result of the Data Breach, Plaintiff Travis Taylor has suffered anxiety due to the public dissemination of his personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his Private Information for purposes of identity theft and fraud. Plaintiff Travis Taylor is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

100. Plaintiff Travis Taylor suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that the Clinics obtained from him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

101. As a result of the Data Breach, Plaintiff Travis Taylor anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, he is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS REPRESENTATION ALLEGATIONS

102. Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose Private Information was accessed in the Data Breach.

Excluded from the Class are the Clinics, their executives and officers, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change or expand the Class definition after conducting discovery.

103. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of the Clinics and obtainable by Plaintiffs only through the discovery process. On information and belief, the number of affected individuals estimated to be 53,916.[30] The members of the Class will be identifiable through information and records in the Clinics' possession, custody, and control.

104. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When the Clinics learned of the Data Breach;

b. Whether hackers obtained Class members' Private Information via the Data Breach;

c. Whether the Clinics' response to the Data Breach was adequate;

[30] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/efa54f35-82e5-40d7-88ab-ca141d9f50ff.html.

d. Whether the Clinics failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether the Clinics knew or should have known that its data security systems and monitoring processes were deficient;

f. Whether the Clinics owed a duty to safeguard their Private Information;

g. Whether the Clinics breached its duty to safeguard Private Information;

h. Whether the Clinics had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

i. Whether the Clinics breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

j. Whether the Clinics' conduct violated the FTCA, HIPAA, and/or the Consumer Protection Act invoked herein;

k. Whether the Clinics' conduct was negligent;

l. Whether the Clinics' conduct was *per se* negligent;

m. Whether the Clinics was unjustly enriched;

n. What damages Plaintiffs and Class members suffered as a result of the Clinics' misconduct;

o. Whether Plaintiffs and Class members are entitled to actual and/or statutory damages; and

p. Whether Plaintiffs and Class members are entitled to additional credit or identity monitoring and monetary relief.

105. Typicality: Plaintiffs' claims are typical of the claims of the Class as Plaintiffs and all members of the Class had their Private Information compromised in the Data Breach. Plaintiffs' claims and damages are also typical of the Class because they resulted from the Clinics' uniform wrongful conduct. Likewise, the relief to which Plaintiffs are entitled to is typical of the Class because the Clinics have acted, and refused to act, on grounds generally applicable to the Class.

106. Adequacy: Plaintiffs are adequate class representatives because their interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, they have retained counsel competent and highly experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Neither Plaintiffs nor their counsel have any interests that are antagonistic to the interests of other members of the Class.

107. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class, a class action is superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by the Clinics' conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, the Clinics' records and databases.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(By Plaintiffs on behalf of the Class)

108. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

109. The Clinics owe a duty of care to protect the Private Information belonging to Plaintiffs and Class members. The Clinics also owe several specific duties including, but not limited to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;

d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class members pursuant to the FTCA;

e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. to promptly notify Plaintiffs and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

110. The Clinics owe this duty because it had a special relationship with Plaintiffs' and Class members. Plaintiffs and Class members entrusted their Private Information to the Clinics on the understanding that adequate security precautions would be taken to protect this information. Furthermore, only the Clinics had the ability to protect its systems and the Private Information stored on them from attack.

111. The Clinics also owe this duty because industry standards mandate that the Clinics protect its patients' confidential Private Information.

112. The Clinics also owe a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiffs and Class members. This duty exists to provide Plaintiffs and Class members with the opportunity to undertake appropriate measures to mitigate

damages, protect against adverse consequences, and thwart future misuse of their Private Information.

113. The Clinics breached their duties owed to Plaintiffs and Class members by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard their Private Information.

114. The Clinics also breached the duties they owed to Plaintiffs and Class members by failing to timely and accurately disclose to them that their Private Information had been improperly acquired and/or accessed.

115. As a direct and proximate result of the Clinics' conduct, Plaintiffs and Class members were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; and
- Permanent increased risk of identity theft.

116. Plaintiffs and Class members were foreseeable victims of any inadequate security practices on the part of the Clinics and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

117. In failing to provide prompt and adequate individual notice of the Data Breach, the Clinics also acted with reckless disregard for the rights of Plaintiffs and Class members.

118. Plaintiffs are entitled to damages in an amount to be proven at trial and injunctive relief requiring the Clinics to, *inter alia*, strengthen its data security systems and monitoring

procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

COUNT II
NEGLIGENCE *PER SE*
(By Plaintiffs on behalf of the Class)

119. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

120. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, imposes a duty on the Clinics to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiffs and Class members.

121. HIPAA imposes a duty on the Clinics to implement reasonable safeguards to protect Plaintiffs' and Class members' Private Information. 42 U.S.C. § 1302(d), *et seq*.

122. HIPAA also requires the Clinics to render unusable, unreadable, or indecipherable all Private Information it collected. The Clinics were required to do so through "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

123. In the event of a data breach, HIPAA obligates Covered Entities and Business Associates to notify affected individuals, prominent media outlets, and the Secretary of the Department of Health and Human Services of the data breach without unreasonable delay and in no event later than 60 days after discovery of the data breach. 45 CFR § 164.400, *et seq*.

124. The Clinics violated the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiffs' and Class members' Private Information.

125. The Clinics violated HIPAA by failing to properly encrypt the Private Information it collected.

126. The Clinics violated HIPAA by unduly delaying reasonable notice of the actual breach; in this case by over three months.

127. The Clinics' failure to comply with HIPAA and the FTCA constitutes negligence *per se*.

128. Plaintiffs and Class members are within the class of persons that the FTCA and HIPAA are intended to protect.

129. It was reasonably foreseeable that the failure to protect and secure Plaintiffs' and Class members' Private Information in compliance with applicable laws and industry standards would result in that Information being accessed and stolen by unauthorized actors.

130. As a direct and proximate result of the Clinics' negligence *per se*, Plaintiffs and Class members have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to theft of their personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased risk of identity theft.

131. Plaintiffs and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring the Clinics to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

COUNT III
BREACH OF IMPLIED CONTRACT
(By Plaintiffs on behalf of the Class)

132. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

133. Plaintiffs and Class members provided the Clinics with their Private Information.

134. By providing their Private Information, and upon the Clinics' acceptance of this information, Plaintiffs and the Class, on one hand, and the Clinics, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

135. The implied contracts between the Clinics and Plaintiffs and Class members obligated the Clinics to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiffs' and Class members' Private Information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above.

136. The implied contracts for data security also obligated the Clinics to provide Plaintiffs and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information.

137. The Clinics breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiffs and Class members; allowing unauthorized persons to access Plaintiffs' and Class members' Private Information; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiffs and Class members, as alleged above.

138. As a direct and proximate result of the Clinics' breaches of the implied contracts, Plaintiffs and Class members have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information, and are entitled to damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(By Plaintiffs on behalf of the Class)

139. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

140. This count is brought in the alternative to Count III.

141. Plaintiff and the Class have a legal and equitable interest in their Private Information that was collected and maintained by the Clinics.

142. Plaintiff and the Class conferred their Private Information to the Clinics as part of receiving medical care. Plaintiff and the Class also conferred payment to the Clinics in exchange for medical services.

143. Plaintiff and Class members conferred their Private Information alongside payment with the understanding that the payment was, in part, to be used to implement data security sufficient to adequately protect their Private Information. And this payment represented a benefit that was to be used for a specific purpose.

144. Clinics received payment from its patients to handle and manage this Private Information. Plaintiff and Class members conferral of their Private Information was a direct benefit since the Clinics were able to use this information for business purposes and financial gain. There was an understanding that a portion of the monies the Clinics received from the use of this Private Information, was intended to be used to implement data security sufficient to adequately protect this Private Information.

145. The Clinics understood that they were so benefitted respectively.

146. However, instead of providing a reasonable level of security, training, protocols, and other measures that would have prevented the Data Breach, as described in detail above, the Clinics, upon information and belief, knowingly and opportunistically elected to increase its own

profits at the expense of Plaintiff and Class members by not expending the money required to do so.

147. And in failing to expend the monies conferred with the express understanding that it would be used on data security, Defendants knowingly and deliberately enriched themselves at the expense of Plaintiff and Class members.

148. Under the common law doctrine of unjust enrichment, it is inequitable for the Clinics to be permitted to retain the benefits they received, and are still receiving, without justification, from Plaintiff and Class members in an unfair and unconscionable manner.

149. The Clinics are therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on the Clinics as a result of their wrongful conduct, including specifically the value to the Clinics of the Private Information that was accessed and exfiltrated in the Data Breach and the profits the Clinics received from the use of that information. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from the Clinics and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by the Clinics from its wrongful conduct.

150. Plaintiffs and Class members may not have an adequate remedy at law against the Clinics, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
BREACH OF FIDUCIARY DUTY
(By Plaintiffs on behalf of the Class)

151. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein

152. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein

153. A fiduciary relationship existed between the Clinics and Plaintiffs and the Class members. Plaintiffs and the Class members placed the Clinics in a position of trust and confidence by providing them with their Private Information as a condition of receiving medical services. The Clinics, in turn, accepted and appreciated this Private Information.

154. The Clinics assumed a fiduciary duty not to disclose the Private Information provided by Plaintiffs and the Class members to unauthorized third parties. Again, the Private Information was confidential, novel, highly personal, and sensitive.

155. This fiduciary duty also arose from the very nature of the patient–physician relationship that existed between the Clinics on one hand and the Plaintiffs and Class members on the other.

156. The Clinics breached the fiduciary duty owed to Plaintiffs and the Class members by failing to act with the utmost good faith, fairness, and honesty, and failing to protect the Private Information in their possession.

157. As a direct and proximate result of the Clinics' conduct, Plaintiffs and Class members have and will suffer damages including:

> (i) the loss of rental or use value of their Private Information;
>
> (ii) the unconsented disclosure of their Private Information to unauthorized third parties;
>
> (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information;
>
> (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft;
>
> (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports;

(vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses;

(vii) the continued risk to their Private Information, which remains in the Clinics' possession and is subject to further unauthorized disclosures so long as the Clinics fail to undertake appropriate and adequate measures to protect it;

(viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives; and

(ix) any nominal damages that may be awarded.

COUNT VI
INVASION OF PRIVACY
(By Plaintiffs on behalf of the Class)

158. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

159. Plaintiffs and Class members had a reasonable expectation of privacy in the Private Information that the Clinics possessed and/or continues to possess.

160. By failing to keep Plaintiffs' and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, the Clinics invaded Plaintiffs' and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiffs and Class members, which is highly offensive to a reasonable person.

161. The Clinics knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' position would consider the Clinics' actions highly offensive.

162. The Clinics invaded Plaintiffs' and Class members' right to privacy and intruded into Plaintiffs' and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

163. As a proximate result of such misuse and disclosures, Plaintiffs' and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. The Clinics' conduct amounted to a serious invasion of Plaintiffs' and Class members' protected privacy interests.

164. In failing to protect Plaintiffs' and Class members' Private Information, and in misusing and/or disclosing their Private Information, the Clinics have acted with malice and oppression and in conscious disregard of Plaintiffs' and Class members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its millions of patients. Plaintiffs, therefore, seek an award of damages, including punitive damages, on behalf of themselves and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all members of the Class, respectfully request that the Court enter judgment in their favor and against the Defendants, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;

B. That Plaintiffs be granted the declaratory relief sought herein;

C. That the Court grant permanent injunctive relief to prohibit the Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

D. That the Court award Plaintiffs and Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiffs and Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

F. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the putative Class, demand a trial by jury on all issues so triable.

Dated: October 31, 2024

Respectfully submitted,

/s/ Domenica M. Russo

Domenica M. Russo – Mo. Bar # 74819
Brandon M. Wise – Mo. Bar #67242
PEIFFER WOLF CARR KANE CONWAY & WISE. LLP
One U.S. Bank Plaza, Suite 1950
St. Louis, MO 63101
Telephone: 314-833-4827
Email: drusso@peifferwolf.com
Email: bwise@peifferwolf.com

Daniel O. Herrera*
Nickolas J. Hagman*
Alex Lee*
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com
alee@caffertyclobes.com

* *Pro Hac Vice* forthcoming

Attorneys for Plaintiffs and the Proposed Class